IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF PENNSYLVANIA

BARBARA GRAY, individually and on behalf of all others similarly situated, Plaintiff, v. GEISINGER HEALTH and NUANCE COMMUNICATIONS, INC., Defendants.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff BARBARY GRAY ("Plaintiff"), individually and on behalf of all others similarly situated, brings this action against Defendants GEISINGER HEALTH ("Geisinger") and NUANCE COMMUNICATIONS, INC. ("Nuance") (collectively "Defendants") and alleges as follows based on personal knowledge as to her own acts and on investigation conducted by counsel as to all other allegations:

PARTIES

1. Plaintiff BARBARA GRAY is a citizen and resident of Centre County, Pennsylvania.

2. Defendant GEISINGER HEALTH is a domestic corporation with its principal place of business in Danville, Pennsylvania.

3. Defendant NUANCE COMMUNICATIONS, INC. is a Delaware corporation with its principal place of business in Burlington, Massachusetts.

JURISDICTION AND VENUE

4. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) because (1) the matter in controversy exceeds the sum or value of

$5,000,000, exclusive of interest and costs, (2) the action is a class action, (3) there are Class members who are diverse from Defendants, and (4) there are more than 100 Class members.

5. This Court has general personal jurisdiction over Defendants because Defendants conduct business in this state.

6. Venue is proper in this district pursuant to 28 U.S.C. § 1391(b)(1) because Geisinger is a resident of this district.

FACTUAL ALLEGATIONS

I. Background

7. Geisinger is among the nation's leading providers of value-based care, serving 1.2 million people in urban and rural communities across Pennsylvania.[1]

8. Geisinger's patients, like Plaintiff and Class members, provided certain Personal Identifying Information ("PII") and Protected Health Information ("PHI") (collectively, "Private Information") to Geisinger, which is necessary to obtain Geisinger's services.

9. Defendant Nuance is a provider of information technology services that works with "77 percent of U.S. hospitals and more than 75 percent of the Fortune 100 companies worldwide."[2]

10. Large companies like Defendants have an acute interest in maintaining the confidentiality of the Private Information entrusted to it, and they are well-aware of the numerous data breaches that have occurred throughout the United States and their responsibility for safeguarding Private Information in its possession.

[1] *See* https://www.geisinger.org/about-geisinger/news-and-media/news-releases/2024/06/24/18/17/geisinger-provides-notice-of-nuances-data-security-incident (last accessed, Jul. 1, 2024).
[2] *See* https://www.linkedin.com/company/nuance-communications (last accessed Jul. 1, 2024).

11. For example, Geisinger represented to consumers and the public that they possess robust security features to protect Private Information and that they take their responsibility to protect Private Information seriously.

12. Geisinger's Privacy Policy states:

> We are required by law to maintain the privacy of protected health information (PHI) and to provide individuals with notice of its legal duties and privacy practices with respect to protected health information.
>
> It's also important to Geisinger Health Plan (GHP) to uphold the trust of our members and those with whom we interact. We are committed to assuring the confidentiality of your PHI.[3]

13. Similarly, Nuance claims that it "collects personal data when [they] deliver [their] products, conduct marketing, and run [their] business operations."[4] Nuance further advises its clients that they "manage[] your data responsibly and respectfully."[5]

14. Nuance's Data Governance Program states:

> As a global leader in conversational AI, clients trust Nuance to deliver solutions that handle patient data responsibly. We remain firmly committed to helping our clients comply with their data protection requirements.

II. The Data Breach

15. According to Geisinger, on November 29, 2023, Geisinger learned that a former Nuance employee accessed Geisinger patient information ("Data Breach").

16. Geisinger announced via press release on June 24, 2024:

> On Nov. 29, 2023, Geisinger discovered and immediately notified Nuance that a former Nuance employee had accessed certain Geisinger patient information two days after the employee had been

[3] *See* https://www.geisinger.org/about-geisinger/corporate/corporate-policies/hipaa/notice-of-privacy-practices-ghp (last accessed Jul. 1, 2024).
[4] *See* https://www.nuance.com/about-us/company-policies/privacy-policies.html (last accessed Jul. 1, 2024).
[5] *See* https://www.nuance.com/about-us/trust-center/privacy.html (last accessed Jul. 1, 2024).

> terminated. Upon learning this, Nuance permanently disconnected its former employee's access to Geisinger's records. An investigation was launched, and law enforcement was engaged. Because it could have impeded their investigation, law enforcement investigators asked Nuance to delay notifying patients of this incident until now. The former Nuance employee has been arrested and is facing federal charges.
>
> Through its investigation, Nuance determined the former employee may have accessed and taken information pertaining to more than one million Geisinger patients.[6]

17. The Data Breach compromised customers' names, dates of birth, addresses, medical record numbers, race, gender, admits and discharges or transfer codes, phone numbers, and facility name abbreviations.[7]

18. The Data Breach affected over one million patients, including Plaintiff and Class members, who entrusted their Private Information to Geisinger.

19. Nuance sent a breach notification letter to affected customers on or around June 21, 2024.

20. Neither Geisinger or Nuance have stated why they were unable to prevent the Data Breach or which security feature failed.

21. Defendants did not state what aspects of the investigation caused them to wait almost seven months after the Data Breach before notifying affected customers.

22. Defendants failed to prevent the Data Breach because they did not adhere to commonly accepted security standards and failed to detect that their databases were subject to a security breach.

III. Plaintiff's Experience

[6] *See* https://www.geisinger.org/about-geisinger/news-and-media/news-releases/2024/06/24/18/17/geisinger-provides-notice-of-nuances-data-security-incident (last accessed Jul. 1, 2024).

[7] *See* Notice Letter addressed to Plaintiff, attached as Ex. A.

23. Plaintiff is very careful about sharing their sensitive Private Information and diligently maintains their Private Information in a safe and secure manner. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

24. As a result of the Data Breach, Plaintiff has and will continue to spend time trying to mitigate the consequences of the Data Breach. This includes time spent verifying the legitimacy of communications related to the Data Breach, and self-monitoring their accounts and credit reports to ensure no fraudulent activity has occurred.

25. Plaintiff has spent multiple hours per day sifting through spam calls and messages, and has spent considerable amount of time attempting to stop such spam communications.

26. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach and has anxiety and increased concerns for the loss of their privacy.

27. This time has been lost forever and cannot be recaptured. The harm caused to Plaintiff cannot be undone.

28. Plaintiff further suffered actual injury in the form of damages to and diminution in the value of their Private Information—a form of intangible property that Plaintiff entrusted to Defendants, which was compromised in and as a result of the Data Breach.

29. Plaintiff has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from their Private Information being placed in the hands of cybercriminals.

30. Future identity theft monitoring is reasonable and necessary and such services will include future costs and expenses.

31. Plaintiff has a continuing interest in ensuring that their Private Information, which, upon information and belief, remains in Defendants' control, is protected, and safeguarded from future breaches.

IV. Injuries to Plaintiff and Class members

32. As a direct and proximate result of Defendants' actions and omissions in failing to protect Plaintiff and Class members' Private Information, Plaintiff and Class members have been injured.

33. Plaintiff and Class members have been placed at a substantial risk of harm in the form of credit fraud or identity theft and have incurred and will likely incur additional damages, including spending substantial amounts of time monitoring accounts and records, in order to prevent and mitigate credit fraud, identity theft, and financial fraud.

34. In addition to the irreparable damage that may result from the theft of Private Information, identity theft victims must spend numerous hours and their own money repairing the impacts caused by a breach. After conducting a study, the Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[8]

35. In addition to fraudulent charges and damage to their credit, Plaintiff and Class members may spend substantial time and expense (a) monitoring their accounts to identify fraudulent or suspicious charges; (b) cancelling and reissuing cards; (c) purchasing credit monitoring and identity theft prevention services; (d) attempting to withdraw funds linked to compromised, frozen accounts; (e) removing withdrawal and purchase limits on compromised accounts; (f) communicating with financial institutions to dispute fraudulent charges; (g) resetting

[8] U.S. Dep't of Justice, *Victims of Identity Theft, 2014* (Nov. 13, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf.

automatic billing instructions and changing passwords; (h) freezing and unfreezing credit bureau account information; (i) cancelling and re-setting automatic payments as necessary; (j) extreme emotional distress and anxiety; and (k) paying late fees and declined payment penalties as a result of failed automatic payments.

36. Additionally, Plaintiff and Class members have suffered or are at increased risk of suffering from, *inter alia*, the loss of the opportunity to control how their Private Information is used, the diminution in the value or use of their Private Information, and the loss of privacy.

V. Securing Private Information and Preventing Breaches

37. Defendants could have prevented this Data Breach by properly securing and encrypting the Private Information of Plaintiff and Class members. Alternatively, Defendants could have destroyed the data they no longer had a reasonable need to maintain or only stored data in an Internet-accessible environment when there was a reasonable need to do so.

38. Defendants' negligence in safeguarding the Private Information of Plaintiff and Class members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

39. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the Private Information of Plaintiff and Class members from being compromised.

40. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[9] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other

[9] 17 C.F.R. § 248.201 (2013).

things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[10]

41. The ramifications of Defendants' failure to keep secure the Private Information of Plaintiff and Class members are long lasting and severe. Once Private Information is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

VI. The Value of Private Information

42. It is well known that Private Information, and social security numbers and financial account information in particular, is an invaluable commodity and a frequent target of hackers.

43. People place a high value not only on their Private Information, but also on the privacy of that data. This is because identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.[11]

44. People are particularly concerned with protecting the privacy of their financial account information and social security numbers, which are the "secret sauce" that is "as good as your DNA to hackers."[12] There are long-term consequences to data breach victims whose social security numbers are taken and used by hackers. Even if they know their social security numbers have been accessed, Plaintiff and Class members cannot obtain new numbers unless they become a victim of social security number misuse. Even then, the Social Security Administration has

[10] *Id*.
[11] Identity Theft Resource Center, *Identity Theft: The Aftermath 2017*, https://www.ftc.gov/system/files/documents/public_comments/2017/10/00004-141444.pdf.
[12] Cameron Huddleston, *How to Protect Your Kids From the Anthem Data Breach*, Kiplinger, (Feb. 10, 2015), https://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html.

warned that "a new number probably won't solve all [] problems . . . and won't guarantee . . . a fresh start."[13]

45. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[14] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[15] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[16]

46. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you

[13] Social Security Admin., *Identity Theft and Your Social Security Number*, at 6-7, https://www.ssa.gov/pubs/EN-05-10064.pdf.
[14] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.
[15] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.
[16] *In the Dark*, VPNOverview, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.

> never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[17]

47. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

48. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[18]

49. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

50. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information,

[17] Social Security Administration, *Identity Theft and Your Social Security Number*, https://www.ssa.gov/pubs/EN-05-10064.pdf.
[18] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft.

personally identifiable information and Social Security numbers are worth more than 10x on the black market."[19]

51. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

52. The fraudulent activity resulting from the Data Breach may not come to light for years.

53. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[20]

54. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class members, including Social Security numbers, and of the foreseeable consequences that would occur if their data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class members as a result of a breach.

55. Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and Class members are

[19] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[20] *Report to Congressional Requesters*, GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

56. Defendants knew of the unique type and the significant volume of data contained in the Private Information that Defendants stored on their networks, and, thus, the significant number of individuals who would be harmed by the exposure of the data.

57. The injuries to Plaintiff and Class members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class members.

VII. Industry Standards for Data Security

58. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[21]

59. In light of the numerous high-profile data breaches targeting companies like Target, Neiman Marcus, eBay, Anthem, Deloitte, Equifax, Marriott, T-Mobile, and Capital One, Defendants knew of the importance of safeguarding Private Information, as well as of the foreseeable consequences of its systems being breached.

60. Therefore, the increase in such attacks, and the attendant risk of future attacks, were widely known to the public and to anyone in Defendants' industry, including Defendants.

61. Security standards commonly accepted among businesses that store Private Information using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Monitoring for suspicious or irregular traffic to servers;

c. Monitoring for suspicious credentials used to access servers;

[21] *How to Protect Your Networks from Ransomware*, FBI, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

d. Monitoring for suspicious or irregular activity by known users;

e. Monitoring for suspicious or unknown users;

f. Monitoring for suspicious or irregular server requests;

g. Monitoring for server requests for Private Information;

h. Monitoring for server requests from VPNs; and

i. Monitoring for server requests from Tor exit nodes.

62. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for cybersecurity[22] and protection of Private Information[23] which includes basic security standards applicable to all types of businesses.

63. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hacker attacks.

[22] Start with Security: A Guide for Business, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
[23] Protecting Personal Information: A Guide for Business, FTC (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting personalinformation.pdf.

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

64. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[24]

65. Because Plaintiff and Class members entrusted Defendants with Private Information, Defendants had a duty to keep the Private Information secure.

[24] Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement.

66. Plaintiff and Class members reasonably expect that when their Private Information is provided to a sophisticated business for a specific purpose, that business will safeguard their Private Information and use it only for that purpose.

67. Nonetheless, Defendants failed to prevent the Data Breach. Had Defendants properly maintained and adequately protected their systems, they could have prevented the Data Breach.

VIII. HIPAA Standards and Violations

68. In addition to failing to follow universal data security practices, Defendants failed to follow healthcare industry standard security practices, including:

a. Failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. 164.306(a)(2);

b. Failing to ensure compliance with HIPAA security standards by their workforce or agents in violation of 45 C.F.R 164.306(a)(94);

c. Failing to effectively train all members of its workforce and its agents on the policies and procedures with respect to PHI as necessary to maintain the security of PHI in violation of C.F.R. 164.530(b) and 45 C.F.R. 164.308(a)(5); and

d. Failing to design and implement and enforce policies and procedures to establish administrative safeguards to reasonably safeguard PHI in compliance with 45 C.F.R. 164.530(c).

CLASS ALLEGATIONS

69. This action is brought as a class action pursuant to Fed. R. Civ. P. 23.

70. The Class is defined as follows:

> **Nationwide Class:** All persons whose Private Information was maintained on Defendants' servers that were compromised in the Data Breach.

71. The Class excludes the following: Defendants, their affiliates, and their current and former employees, officers and directors, and the Judge assigned to this case.

72. The Class definition may be modified, changed, or expanded based upon discovery and further investigation.

73. *Numerosity*: The Class is so numerous that joinder of all members is impracticable, evidenced by the large number of individuals presently known to have been injured by Defendants' conduct. The Class is ascertainable by records in the possession of Defendants or third parties.

74. *Commonality*: Questions of law or fact common to the Class include, without limitation:

a. Whether Defendants owed a duty or duties to Plaintiff and Class members to exercise due care in collecting, storing, safeguarding, and obtaining their Private Information;

b. Whether Defendants breached that duty or those duties;

c. Whether Defendants failed to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records to protect against known and anticipated threats to security;

d. Whether the security provided by Defendants was satisfactory to protect Private Information as compared to industry standards;

e. Whether Defendants misrepresented or failed to provide adequate information regarding the type of security practices used;

f. Whether Defendants knew or should have known that they did not employ reasonable measures to keep Plaintiff and Class members' Private Information secure and prevent loss or misuse of that Private Information;

g. Whether Defendants acted negligently in connection with the monitoring and protecting of Plaintiff and Class members' Private Information;

h. Whether Defendants' conduct was intentional, willful, or negligent;

i. Whether Plaintiff and Class members suffered damages as a result of Defendants' conduct, omissions, or misrepresentations; and

j. Whether Plaintiff and Class members are entitled to injunctive, declarative, and monetary relief as a result of Defendants' conduct.

75. *Typicality*: Plaintiff's claims are typical of the claims of Class members. Plaintiff and Class members were injured and suffered damages in substantially the same manner, have the same claims against Defendants relating to the same course of conduct, and are entitled to relief under the same legal theories.

76. *Adequacy*: Plaintiff will fairly and adequately protect the interests of the Class and have no interests antagonistic to those of the Class. Plaintiff's counsel are experienced in the prosecution of complex class actions, including actions with issues, claims, and defenses similar to the present case.

77. *Predominance and superiority*: Questions of law or fact common to Class members predominate over any questions affecting individual members. A class action is superior to other available methods for the fair and efficient adjudication of this case because individual joinder of all Class members is impracticable and the amount at issue for each Class member would not justify the cost of litigating individual claims. Should individual Class members be required to bring separate actions, this Court would be confronted with a multiplicity of lawsuits burdening the court system while also creating the risk of inconsistent rulings and contradictory judgments. In contrast to proceeding on a case-by-case basis, in which inconsistent results will magnify the delay and expense to all parties and the court system, this class action presents far fewer management difficulties while providing unitary adjudication, economies of scale and comprehensive supervision by a single court. There are no known difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

78. Accordingly, this class action may be maintained pursuant to Fed. R. Civ. P. 23(b)(3).

79. Defendants' unlawful conduct applies generally to all Class members, thereby making appropriate final equitable relief with respect to the Class as a whole.

80. Accordingly, this class action may be maintained pursuant to Fed. R. Civ. P. 23(b)(2).

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(on behalf of the Class)

81. All preceding paragraphs are incorporated herein by reference as though fully set forth herein.

82. Defendants owed a duty of care to Plaintiff and Class members to use reasonable means to secure and safeguard the entrusted Private Information, to prevent its unauthorized access and disclosure, to guard it from theft, and to detect any attempted or actual breach of its systems. These common law duties existed because Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiff and Class members would be harmed by the failure to protect their Private Information because hackers routinely attempt to steal such information and use it for nefarious purposes, but Defendants knew that it was more likely than not Plaintiff and Class members would be harmed by such exposure of their Private Information.

83. Defendants' duties to use reasonable security measures also arose as a result of the special relationship that existed between Defendants, on the one hand, and Plaintiff and Class members, on the other hand. The special relationship arose because Plaintiff and Class members entrusted their Private Information with Defendants, Defendants accepted and held the Private Information, and Defendants represented that the Private Information would be kept secure

pursuant to their data security policies. Defendants could have ensured that their data security systems and practices were sufficient to prevent or minimize the data breach.

84. Defendants' duties to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect Private Information. Various FTC publications and data security breach orders further form the basis of Defendants' duties. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

85. Defendants' violations of Section 5 of the FTC Act constitute negligence per se.

86. Defendants breached the aforementioned duties when they failed to use security practices that would protect Plaintiff and Class members' Private Information, thus resulting in unauthorized third-party access to the Plaintiff and Class members' Private Information.

87. Defendants further breached the aforementioned duties by failing to design, adopt, implement, control, manage, monitor, update, and audit their processes, controls, policies, procedures, and protocols to comply with the applicable laws and safeguard and protect Plaintiff and Class members' Private Information within their possession, custody, and control.

88. As a direct and proximate cause of failing to use appropriate security practices, Plaintiff and Class members' Private Information was disseminated and made available to unauthorized third parties.

89. Defendants admitted that Plaintiff and Class members' Private Information was wrongfully disclosed as a result of the breach.

90. The breach caused direct and substantial damages to Plaintiff and Class members, as well as the possibility of future and imminent harm through the dissemination of their Private Information and the greatly enhanced risk of credit fraud or identity theft.

91. By engaging in the forgoing acts and omissions, Defendants committed the common law tort of negligence. For all the reasons stated above, Defendants' conduct was negligent and departed from reasonable standards of care including by, but not limited to: failing to adequately protect the Private Information; failing to conduct regular security audits; and failing to provide adequate and appropriate supervision of persons having access to Plaintiff and Class members' Private Information.

92. But for Defendants' wrongful and negligent breach of its duties owed to Plaintiff and Class members, their Private Information would not have been compromised.

93. Neither Plaintiff nor the Class contributed to the breach or subsequent misuse of their Private Information as described in this Complaint.

94. As a direct and proximate result of Defendants' actions and inactions, Plaintiff and Class members have been put at an increased risk of credit fraud or identity theft, and Defendants must mitigate damages by providing adequate credit and identity monitoring services.

95. Plaintiff and Class members are entitled to damages for the reasonable costs of future credit and identity monitoring services for a reasonable period of time, substantially in excess of one year.

96. Plaintiff and Class members are entitled to damages to the extent that they have directly sustained damages as a result of identity theft or other unauthorized use of their Private Information, including the amount of time Plaintiff and Class members have spent and will continue to spend as a result of Defendants' negligence.

97. Plaintiff and Class members are entitled to damages to the extent their Private Information has been diminished in value because Plaintiff and Class members no longer control their Private Information and to whom it is disseminated.

COUNT II
BREACH OF IMPLIED CONTRACT
(on behalf of the Class)

98. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

99. Defendants invited Plaintiff and Class members to provide their Private Information to Defendants. As consideration for the benefits Defendants provided, Plaintiff and Class members provided their Private Information to Defendants. When Plaintiff and Class members provided their Private Information to Defendants, they entered into implied contracts by which Defendants agreed to protect their Private Information and only use it solely to administer benefits. As part of the offer, Defendants would safeguard the Private Information using reasonable or industry-standard means.

100. Accordingly, Plaintiff and Class members accepted Defendants' offer to administer benefits and provided Defendants their Private Information.

101. Plaintiff and Class members fully performed their obligations under the implied contracts with Defendants. However, Defendants breached the implied contracts by failing to safeguard Plaintiff's and the Class's Private Information.

102. The losses and damages Plaintiff and Class members sustained that are described herein were the direct and proximate result of Defendants' breaches of its implied contracts with them. Additionally, because Plaintiff and Class members continue to be parties to the ongoing administration and distribution of benefits under the contracts, and because damages may not provide a complete remedy for the breaches alleged herein, Plaintiff and Class members are

therefore entitled to specific performance of the contracts to ensure data security measures necessary to properly effectuate the contracts maintain the security of their Private Information from unlawful exposure.

103. Defendants' conduct as alleged herein also violated the implied covenant of good faith and fair dealing inherent in every contract, and Plaintiff and Class members are entitled to associated damages and specific performance.

COUNT III
UNJUST ENRICHMENT
(on behalf of the Class)

104. All preceding paragraphs are incorporated herein by reference as though fully set forth herein.

105. Plaintiff and Class members have an interest, both equitable and legal, in their Private Information that was conferred upon, collected by, and maintained by Defendants and that was ultimately compromised in the data breach.

106. Defendants, by way of their acts and omissions, knowingly and deliberately enriched themselves by saving the costs they reasonably should have expended on security measures to secure Plaintiff and Class members' Private Information.

107. Defendants also understood and appreciated that the Private Information pertaining to Plaintiff and Class members was private and confidential and its value depended upon Defendants maintaining the privacy and confidentiality of that Private Information.

108. Instead of providing for a reasonable level of security that would have prevented the breach—as is common practice among companies entrusted with such Private Information—Defendants instead consciously and opportunistically calculated to increase their own profits at the expense of Plaintiff and Class members. Nevertheless, Defendants continued to obtain the benefits conferred on them by Plaintiff and Class members. The benefits conferred upon, received,

and enjoyed by Defendants were not conferred gratuitously, and it would be inequitable and unjust for Defendants to retain these benefits.

109. Plaintiff and Class members, on the other hand, suffered as a direct and proximate result. As a result of Defendants' decisions to profit rather than provide requisite security, and the resulting breach disclosing Plaintiff and Class members' Private Information, Plaintiff and Class members suffered and continue to suffer considerable injuries in the forms of, *inter alia*, attempted identity theft, time and expenses mitigating harms, diminished value of Private Information, loss of privacy, and increased risk of harm.

110. Thus, Defendants engaged in opportunistic conduct in spite of its duties to Plaintiff and Class members, wherein they profited from interference with Plaintiff and Class members' legally protected interests. As such, it would be inequitable, unconscionable, and unlawful to permit Defendants to retain the benefits it derived as a consequence of its conduct.

111. Accordingly, Plaintiff and Class members respectfully request that this Court award relief in the form of restitution or disgorgement in the amount of the benefit conferred on Defendants as a result of their wrongful conduct, including specifically, the amounts that Defendants should have spent to provide reasonable and adequate data security to protect Plaintiff and Class members' Private Information, and compensatory damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for a judgment as follows:

a. For an order certifying the Class, appointing Plaintiff as Class Representative, and appointing the law firms representing Plaintiff as counsel for the Class;

b. For compensatory, punitive, statutory, and treble damages in an amount to be determined at trial;

c. Payment of costs and expenses of suit herein incurred;

d. Both pre-and post-judgment interest on any amounts awarded;

e. Payment of reasonable attorneys' fees and expert fees;

f. Such other and further relief as the Court may deem proper.

JURY DEMAND

Trial by jury is demanded.

Dated: July 2, 2024

Respectfully submitted,

/s/ Charles E. Schaffer

Charles E. Schaffer
LEVIN SEDRAN & BERMAN, LLP
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Tel: 215-592-1500
Fax: 215-592-4663
cschaffer@lfsblaw.com

Jeffrey S. Goldenberg
GOLDENBERG SCHNEIDER, LPA
4445 Lake Forest Drive, Suite 490
Cincinnati, OH 45242
Tel: (513) 345-8291
jgoldenberg@gs-legal.com
(Pro hac vice to be filed)

Brett R. Cohen, Esq.
LEEDS BROWN LAW, P.C.
One Old Country Road - Suite 347
Carle Place, NY 11514
Tel: 516-873-9550
bcohen@leedsbrownlaw.com
(Pro hac vice to be filed)

Counsel for Plaintiff and Proposed Class